Math 342: Algebra, Coding Theory and Cryptography
Spring Term, 2009

Lior Silberman

v1.2 (March 15, 2009)

Main Course Website	`http://www.math.ubc.ca/~lior/teaching/342_S09/`
Contact me at	MAT 229B — 604-827-3031 – `lior@math.ubc.ca`
My Website	`http://www.math.ubc.ca/~lior/`
Class	MWF 11-12 at Chemistry Building room 124
Office Hours	Tuesadys 16-17:30, Fridays 13:30-15:00 & by appointment.
Required Textbook	Childs, *A Concrete Introduction to Higher Algebra*
Course Prerequisties	(MATH 152 or 221 or 223) and (MATH 220 or 226 or CPSC 121)

About the course

This course will cover basic elements of abstract algebra, a foundational topic of mathematics:

- Finite rings and fields
- Polynomials and vector spaces over finite fields
- Finite groups

The theoretical material will be developed from its roots in the ordinary arithmetic of the integers and will be illustrated with its applications which underly our modern technological world. Over the last 60 years, methods for communication of information have been predominantly constructed using algebraic structures. We will look at two basic communication problems, and some methods to solve them as an example of applied algebra:

1. Cryptography: how do you transmit private information across a public channel?
   (a) Symmetric cryptography;
   (b) Diffie-Hellman key exchange;
   (c) The RSA cryptosystem.
2. Error detection and correction: how do you transmit information across a noisy channel?
   (a) Checksums. This is how websites can tell if you mistype a digit in your credit card number.
   (b) CRC. This is how your hard-drive can detect failures.
   (c) Linear codes. This is how NASA probes can send low-power transmissions back to Earth.

Teaching and learning

Learning goals

- Developing facility with algebraic structures and abstract algebraic reasoning.
- Developing computational skills in new settings: finite groups, fields and vector spaces.
- Learning to work with formal definitions.
- Connecting mathematics and technology.
- Reading a recent mathematical paper.

What you can expect from me

- To come prepared for class: knowing what we want to achieve, and how we will achieve it.
- Various approaches to the material including lecturing, classroom discussion and groupwork.
- Responses to your questions and concerns: continuously in class and during my office hours, within reasonable time by e-mail outside class.
- Timely and clear explanations of what is correct in your work and what is not, and how you can improve.

What's expected from you

- Come prepared to class, having read the relevant material in the textbook
- Actively participate in the course: do the reading, think about the material, and then ask questions.
- Asking questions when you don't understand, or want to learn more: most importantly in class; but also during office hours. Also, ask your colleagues questions outside of class – you will both benefit from the discussion!
- Thinking hard about assigned problem and about the ideas we will see in class. Working on the problem sets is *absolutely essential* for learning the material. **It is extremely rare for students who skip problem sets to do well on exams.**
- Written work that is readable and communicates your ideas.

Official Policies

Learning

- For every week after the first, there will be assigned pre-class reading (usually from the textbook). The discussions in class will assume that you have read these chapters beforehand. Your main goals are to ***work through the examples*** and become ***familiar with the vocabulary and notations*** we will use, as well as think about the ***ideas*** behind the proofs. Learning the details of the proofs will not be the point.
- Some of the assigned problems will be based on this prospective material.

Assessment

- Written work should be presented carefully, in complete English sentences, and with sufficient detail. A "correct sequence of formulas" will only merit partial credit. Both homework and exams will be divided roughly evenly between calculational and theoretical problems. Examples of the expectations will be distributed together with the first problem set.
- There will be twelve weekly problem sets, due by the end of class a week after they were assigned. I will drop the lowest two scores before calculating the homework grade.
  - Late assignments will not be accepted for credit. In exceptional circumstances (a proof of the emergency and advance notification if possible will be required) a late problem set will be registered (that is, will not be scored a zero) if you finish it and hand it in after the emergency has passed.
  - You are encouraged to work on solving the problems together. However, each of you must write your solutions independently, in your own words. You may (and should) share your ideas but you may not share your written work.
  - It is possible that only certain problems from a problem set will be selected for grading. Complete solutions will be posted in any case.
- There will be a midterm exam in class on Friday morning, Feb. 13th.
  - If you need special accommodations when taking written exams, please contact the Office of Access & Diversity (`access.diversity@ubc.ca`).
  - If the midterm (or final) exam conflicts with a religious observance, please contact me *at least two weeks ahead of time* so we can make appropriate arrangements..
- There will be a final exam during the usual exam period.
- The final grade will be calculated as follows:

Problem sets: 20%
Midterm: 20%
Final exam: 60%

References

[Childs] Childs: *A Concrete Introduction to Higher Algebra, 2^{nd} edition.* Springer-Verlag, New York, 1995. xvi+522 pp. ISBN: 90387-98999-4 (softcover) 0-387-94484-2 (hardcover).

[RSA] Rivest, Shamir and Adleman: *A method for obtaining digital signatures and public-key cryptosystems.* Communications of the ACM **21** (1978), no. 2, 120–126.

The material of the course is standard, and covered by many textbooks. Any book titled "abstract algebra", for example, will contain all the theoretical material. I will also distribute my lecture notes.

Tentative Schedule of Lectures & Readings

The following is accurate as of the date on the front of this syllabus; changes will be announced in class and posted to the course website. Note that the reading is to be done *ahead* of the relevant classes.

1 5/1– 9/1

General introduction; A taste of abstract algebra: the field with two elements, linear algebra over $\mathbb{F}_2$.
The integers: induction.

2 12/1 – 16/1

The integers: division and divisibility, gcd and lcm, Euclid's algorithm.
Reading: [Childs, §§2.A-E, §3.A-B]

3 19/1 – 23/1

Unique factorization, primes, irrational numbers.
Reading: [Childs, §3.C, §4.A-B]

4 26/1 – 30/1

Congruences.
Reading: [Childs, §5.ABDE]

5 2/2 – 6/2

Arithmetic mod m.
Check digits (Credit card numbers, SIN, ISBN, UPC).
Reading: [Childs, §6.A-E]

6 9/2 – 13/2

RSA
Midterm exam on Friday.
Reading: [RSA], [Childs, §10.B]

(16/2 – 20/2 — Midterm break)

7 23/2 – 27/2

Rings and fields.
Reading: [Childs, §8.A-C]

8 2/3 – 6/3

Vector spaces over finite fields.
Reading: Your Linear Algebra textbook.

9 9/3 – 13/3

Subspaces.
Linear codes.
Reading: [Childs, §13.A-E]

10 16/3 – 20/3

Polynomials over finite fields.
CRC.
Reading: [Childs, §§14-15]

11 23/3 – 27/3

Finite groups.
Groups, subgroups, homomorphisms. Normal subgroups and kernels.
Reading: [Childs, §11]

12 30/3 – 2/4

Cosets and Lagrange's Theorem.

13 6/4 – 8/4

Group actions and the symmetric group.